THE TATE MODULE

Seminar: Elliptic curves and the Weil conjecture

Yassin Mousa

Abstract

This paper refers to the 10th talk in the seminar “Elliptic curves and the Weil conjecture” supervised by Prof. Dr. Moritz Kerz at the University of Regensburg in SS2016. In the first part of the paper we will very roughly recall the basic properties of the \( p \)-adic numbers. In the second part we will introduce the Tate module and revisit the group of all isogenies between two elliptic curves.

1 \( p \)-adic Numbers

Definition 1.1. Let \( p \) be a prime number. The ring of \( p \)-adic numbers is the ring

\[ \mathbb{Z}_p := \lim_{\leftarrow n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}, \]

where we take the projective limit with respect to the natural maps

\[ \varphi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \]

\[ 1 \longmapsto 1. \]

Proposition 1.2. Let \( p \) be a prime number, then the ring \( \mathbb{Z}_p \) of \( p \)-adic numbers is integral.

Proof. We use the identification

\[ \mathbb{Z}_p \cong \left\{ ([x_n])_{n \in \mathbb{N}} \in \prod_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \mid \varphi_n([x_{n+1}]) = [x_n] \text{ for all } n \in \mathbb{N} \right\}. \]

We note, that the condition \( \varphi_n([x_{n+1}]) = [x_n] \) is equivalent to \( x_{n+1} \equiv x_n \mod p^n \), therefore \( x_{m+n} \equiv x_n \mod p^n \) for all natural numbers \( m \).
Let $([a_n])_{n \in \mathbb{N}}$ and $([b_n])_{n \in \mathbb{N}}$ be elements of $\mathbb{Z}_p \setminus \{0\}$. We find integers $n, m \in \mathbb{N}$ such that

$$a_m \not\equiv 0 \mod p^m \quad \text{and} \quad b_n \not\equiv 0 \mod p^n.$$ 

Then

$$a_{m+n} \cdot b_{m+n} \not\equiv 0 \mod p^{n+m},$$

because otherwise $p^m$ divides $a_{m+n}$ or $p^n$ divides $b_{m+n}$, which implies that $p^m$ divides $a_m$ or $p^n$ divides $b_n$. Therefore $([a_n]) \cdot ([b_n]) \neq 0$. ■

**Definition 1.3.** Let $p$ be a prime number. We call the quotient field of $\mathbb{Z}_p$

$$\mathbb{Q}_p := \text{Quot}(\mathbb{Z}_p)$$

the field of $p$-adic numbers.

**Proposition 1.4.** Let $p$ be a prime number. Then $\mathbb{Z}_p$ has characteristic 0. Especially $\mathbb{Q}_p$ has characteristic 0.

**Proof.** We have a natural map

$$\mathbb{Z} \rightarrow \mathbb{Z}_p$$

$$z \mapsto ([z])_{n \in \mathbb{N}}.$$ 

This map is injective, thus $\text{char}(\mathbb{Z}_p) = \text{char}(\mathbb{Z}) = 0$. ■

## 2 The Tate Module

Let $E/K$ be an elliptic curve and let $m \geq 2$ be an integer, prime to $\text{char}(K)$ if $\text{char}(K) > 0$. As we have seen we have an isomorphism of abstract groups

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$ 

However, $E[m]$ carries more structure than an abstract group.

We recall that the absolute Galois group $\text{Gal}(\bar{K}/K)$ of $K$ acts on $\bar{K}^\times$ in the category of groups (compare appendix). If $\sigma$ is an element of $\text{Gal}(\bar{K}/K)$ and $k$ is an element of $\bar{K}^\times$ then the action of $\sigma$ on $k$ is simply given by

$$k^\sigma := \sigma(k).$$

Further $\text{Gal}(\bar{K}/K)$ acts on a projective variety over $K$ by acting on its homogeneous coordinates. Moreover on the elliptic curve $E$ this action commutes with the addition
on $E$, therefore $\text{Gal}(\bar{K}|K)$ acts on the group $E$. Then, if $P$ is an element of $E[m]$ and $\sigma$ is an element of $\text{Gal}(\bar{K}|K)$, we find

$$[m]P^\sigma = ([m]P)^\sigma = 0.$$ 

Therefore $\text{Gal}(\bar{K}|K)$ also acts on the group $E[m]$ and this action yields a group homomorphism

$$\text{Gal}(\bar{K}|K) \longrightarrow \text{Aut}(E[m])$$

$$\sigma \longmapsto (P \mapsto P^\sigma)$$

from the absolute Galois group to the automorphism group of $E[m]$. We can choose a basis for $E[m]$ and get an isomorphism

$$\text{Aut}(E[m]) \cong \text{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

It turns out that, individually for each $m$, these representations are not completely satisfactory, since it is generally easier to deal with representations whose matrices have coefficients in a ring with characteristic 0. Heuristically speaking we will use these mod $m$ representations to approximate a characteristic 0 representation.

**Definition 2.1.** Let $E$ be an elliptic curve and let $l \in \mathbb{Z}$ be a prime. The $(l\text{-adic})$ Tate module of $E$ is the group

$$T_l(E) := \lim_{\longleftarrow n \in \mathbb{N}} E[l^n],$$

where we take the projective limit with respect to the natural maps

$$E[l^{n+1}] \overset{l}{\longrightarrow} E[l^n].$$

Each $E[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module by [Sil86, III.6.4b,c] and the scalar multiplication commutes with the multiplication-by-$l$-maps, i.e we have a commutative diagram

$$\begin{array}{ccc}
\mathbb{Z}/l^{n+1}\mathbb{Z} \times E[l^{n+1}] & \longrightarrow & E[l^{n+1}] \\
\downarrow & & \downarrow \overset{l}{\longrightarrow} \\
\mathbb{Z}/l^n\mathbb{Z} \times E[l^n] & \longrightarrow & E[l^n]
\end{array}$$

Hence, $T_l(E)$ has a natural structure as a $\mathbb{Z}_l$-module via the operation

$$\mathbb{Z}_l \times T_l(E) \longrightarrow T_l(E)$$

$$(x_n)_{n \in \mathbb{N}}, (P_n)_{n \in \mathbb{N}} \longmapsto (x_n P_n)_{n \in \mathbb{N}}.$$ 

We can specify the $\mathbb{Z}_l$-module structure of $T_l(E)$ with the following proposition.
Proposition 2.2. As a $\mathbb{Z}_l$-module, the Tate module has the following structure:

1.) $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ if $l \neq \text{char}(K)$,

2.) $T_p(E) \cong \{0\}$ or $\mathbb{Z}_p$ if $p = \text{char}(K) > 0$.

Proof. By theorem [Sil86, III.6.4b,c] we have

1.) $E[l^n] \cong \mathbb{Z}/l^n \mathbb{Z} \times \mathbb{Z}/l^n \mathbb{Z}$ if $l \neq \text{char}(K)$,

2.) $E[p^n] \cong \{0\}$ or $\mathbb{Z}/p^n \mathbb{Z}$ if $p = \text{char}(K) > 0$.

In the case $l \neq \text{char}(K)$ we obtain the commutative diagram

$$
\begin{array}{ccc}
E[l^{n+1}] & \xrightarrow{\phi_{n+1}} & \mathbb{Z}/l^{n+1} \mathbb{Z} \times \mathbb{Z}/l^{n+1} \mathbb{Z} \\
\downarrow{l} & & \downarrow{\varphi_n} \\
E[l^n] & \xrightarrow{\phi_n} & \mathbb{Z}/l^n \mathbb{Z} \times \mathbb{Z}/l^n \mathbb{Z}
\end{array}
$$

where the $\phi_i$’s denote arbitrary isomorphisms from $E[l^i]$ to $\mathbb{Z}/l^i \mathbb{Z} \times \mathbb{Z}/l^i \mathbb{Z}$ and

$$\varphi_n := \phi_n \circ [l] \circ \phi_{n+1}^{-1}.$$

By [Sil86, III.4.2] and [Sil86, II.3] the multiplication-by-$l$-maps are surjective. Let $x_1$ be an arbitrary preimage of $y_1 := \phi_n^{-1}((1, 0)))$ and let $x_2$ be an arbitrary preimage of $y_2 := \phi_n^{-1}((0, 1)))$. The ring $\mathbb{Z}/(l)^{n+1} \mathbb{Z}$ is a local ring with maximal ideal $(l)$. Further under the identification $E[l^{n+1}]/(l) \cong E[l^n]/(l) \cong E[l]$ the residue classes of the $x_i$’s in $E[l]$ correspond to the ones of the $y_i$’s. Hence, by Nakayamas lemma we derive that $\{y_1, y_2\}$ is a generating system of $E[l^{n+1}]$. It is clear that $y_1$ and $y_2$ are linearly independent and we derive that $\{y_1, y_2\}$ is a basis of $E[l^{n+1}]$.

Now we can assume with out loss of generality that $\varphi_n$ is of the form

$$\mathbb{Z}/l^{n+1} \mathbb{Z} \times \mathbb{Z}/l^{n+1} \mathbb{Z} \rightarrow \mathbb{Z}/l^n \mathbb{Z} \times \mathbb{Z}/l^n \mathbb{Z}

(1, 0) \mapsto (1, 0)

(0, 1) \mapsto (0, 1).$$

or otherwise replace $\phi_{n+1}$ by the isomorphism which sends $(1, 0)$ to $x_1$ and $(0, 1)$ to $x_2$. A simple induction on $n$ shows that with out loss of generality we can assume for all $n$ that $\varphi_n$ is of the above form.

Taking projective limits gives us a group isomorphism

$$\varprojlim_n \phi_n : T_l(E) \rightarrow \varprojlim_n \mathbb{Z}/l^n \mathbb{Z} \times \mathbb{Z}/l^n \mathbb{Z} \cong \varprojlim_n \mathbb{Z}/l^n \mathbb{Z} \times \varprojlim_n \mathbb{Z}/l^n \mathbb{Z} \cong \mathbb{Z}_l \times \mathbb{Z}_l.$$

and we obtain the claimed isomorphism.

Claim ii.) can be proven analogously. $lacksquare$
For all natural numbers $n$ the absolute Galois group $\text{Gal}(\overline{K}|K)$ acts on $E[l^n]$ and the action commute with the multiplication-by-$l$-maps. Therefore the absolute Galois group of $K$ acts on $T_l(E)$ via the operation

$$\rho_l : \text{Gal}(\overline{K}|K) \times T_l(E) \to T_l(E)$$

$$(\sigma, (P_n)_n) \mapsto (\sigma P_n)_n$$

and we obtain a group homomorphism

$$\rho_l : \text{Gal}(\overline{K}|K) \to \text{Aut}(T_l(E)).$$

**Definition 2.3.** We call $\rho_l$ the $l$-adic representation (of $\text{Gal}(\overline{K}|K)$ associated to $E$).

**Remark.** Let $l \neq \text{char}(K)$ be a prime. We have an isomorphism $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$. If we choose a $\mathbb{Z}_l$-basis for $T_l(E)$, we obtain a representation

$$\text{Gal}(\overline{K}|K) \to \text{GL}_2(\mathbb{Z}_l)$$

and the natural inclusion $\mathbb{Z}_l \subset \mathbb{Q}_l$ gives us a representation

$$\text{Gal}(\overline{K}|K) \to \text{GL}_2(\mathbb{Q}_l).$$

In this way we obtain a representation of $\text{Gal}(\overline{K}|K)$ over a field of characteristic zero.

The Tate module is a useful tool for studying isogenies. Let

$$\phi : E_1 \to E_2$$

be an isogeny of elliptic curves. Then $\phi$ induces maps

$$\phi_n : E_1[l^n] \to E_2[l^n].$$

Taking projective limits gets us a unique map

$$\lim_{\leftarrow n} \phi_n =: \phi_l : T_l(E_1) \to T_l(E_2).$$

We thus obtain a natural group homomorphism

$$\text{Hom}(E_1, E_2) \to \text{Hom}(T_l(E_1), T_l(E_2))$$

$$\phi \mapsto \phi_l.$$ 

Further, if $E_1 = E_2 = E$, then the map

$$\text{End}(E) \to \text{End}(T_l(E))$$

$$\phi \mapsto \phi_l.$$ 

is even a homomorphism of rings.

The following theorem will give us some strong information of the structure of $\text{Hom}(E_1, E_2)$. 

5
**Theorem 2.5.** Let $E_1$ and $E_2$ be elliptic curves and let $l \neq \text{char}(K)$ be a prime. Then the natural map

$$
\text{Hom}(E_1, E_2) \otimes \mathbb{Z}_l \rightarrow \text{Hom}(T_l(E_1), T_l(E_2))
$$

with

$$
\phi = \sum_i \phi_i \otimes z_i \mapsto \sum_i z_i \phi_i, l =: \phi_l.
$$

is injective.

For the proof of the theorem we need the following lemma.

**Lemma 2.6.** Let $M \subseteq \text{Hom}(E_1, E_2)$ be a finitely generated subgroup, and let

$$M^{\text{div}} := \{ \phi \in \text{Hom}(E_1, E_2) \mid [m] \circ \phi \in M \text{ for some integer } m \geq 1 \}.$$

Then $M^{\text{div}}$ is finitely generated.

**Proof.** By theorem [Sil86, III.4.2b] $\text{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module. Thus $M$ is torsion-free and the fundamental theorem of finitely generated abelian groups implies that $M$ is a free group. Let $\{\beta_1, \ldots, \beta_n\}$ be a $\mathbb{Z}$-basis of $M$. As an $\mathbb{R}$-vector space $M \otimes \mathbb{Z} \mathbb{R}$ is generated by $\{\beta_1 \otimes 1, \ldots, \beta_n \otimes 1\}$. We endow $M \otimes \mathbb{Z} \mathbb{R}$ with the topology, inherited from the standard topology on $\mathbb{R}^n$ via the identification $M \otimes \mathbb{Z} \mathbb{R} \cong \mathbb{R}^n$.

A torsion-free abelian group is always flat (compare [Bou72, §2, 4, Prop.3]). Therefore $\mathbb{R}$ is a flat $\mathbb{Z}$-module and from the inclusion $M \subseteq M^{\text{div}}$ we get an injective map

$$M \otimes \mathbb{Z} \mathbb{R} \hookrightarrow M^{\text{div}} \otimes \mathbb{Z} \mathbb{R}$$

$$\phi \otimes x \mapsto \phi \otimes x.$$

This map is also surjective.

**Because:** We consider an element of the form $\phi \otimes r$ in $M^{\text{div}} \otimes \mathbb{Z} \mathbb{R}$. We find an integer $m \geq 1$ such that $[m] \phi$ lies in $M$. Therefore the element $m \phi \otimes \frac{1}{m} \in M \otimes \mathbb{Z} \mathbb{R}$ is a preimage of $\phi \otimes r$.

Furthermore $M^{\text{div}}$ is flat and thus we obtain an injective map

$$M^{\text{div}} \cong M^{\text{div}} \otimes \mathbb{Z} \mathbb{R} \hookrightarrow M^{\text{div}} \otimes \mathbb{Z} \mathbb{R} \cong M \otimes \mathbb{Z} \mathbb{R}.$$

Hence, we have a natural inclusion

$$M^{\text{div}} \subseteq M \otimes \mathbb{Z} \mathbb{R}.$$

Now we want to extend the degree mapping on $M$ to $M \otimes \mathbb{Z} \mathbb{R}$. Therefore we would like to express the degree mapping on $M$ in terms of the degree of the basis elements.
By [Sil86, III.6.3] we know that the degree map on $\text{Hom}(E_1, E_2)$ is a positive definite quadratic form. Hence, 

$$\langle \alpha, \beta \rangle := \deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta)$$

is bilinear. We find

$$\frac{1}{2} \langle \phi, \phi \rangle = \frac{1}{2} \left( \deg([2] \circ \phi) - 2 \deg(\phi) \right)$$

$$= \frac{1}{2} \left( \deg([2]) \deg(\phi) - 2 \deg(\phi) \right)$$

$$= \frac{1}{2} \left( 4 \deg(\phi) - 2 \deg(\phi) \right)$$

$$= \deg(\phi).$$

Thus if

$$\phi = \sum_{i=1}^{n} a_i \beta_i$$

is an arbitrary element of $M$ we have

$$\deg(\phi) = \frac{1}{2} \left( \sum_{i=1}^{n} a_i \beta_i, \sum_{j=1}^{n} a_i \beta_i \right) = \frac{1}{2} \sum_{i,j} a_i a_j \langle \beta_i, \beta_j \rangle.$$

Therefore

$$\deg : M \otimes_{\mathbb{Z}} \mathbb{R} \longrightarrow \mathbb{R}$$

$$\sum_{i} x_i (\beta_i \otimes 1) \longmapsto \frac{1}{2} \sum_{i,j} x_i x_j \langle \beta_i, \beta_j \rangle$$

extends the degree map, and this extension is clearly continuous.

Then

$$U := \{ \phi \in M \otimes_{\mathbb{Z}} \mathbb{R} \mid \deg(\phi) < 1 \}$$

is an open neighbourhood of 0.

Since every nonzero isogeny has degree at least one we find

$$M^{\text{div}} \cap U = \{0\}.$$ 

So far we have shown that $M^{\text{div}}$ is a discrete subgroup of the finite dimensional $\mathbb{R}$-vector space $M \otimes_{\mathbb{Z}} \mathbb{R}$. From the following general result it follows that $M^{\text{div}}$ is finitely generated.

**Lemma 2.7.** Let $V$ be a finite $n$-dimensional $\mathbb{R}$-vector space endowed with the standard topology of $\mathbb{R}^n$. If $G$ is a discrete subgroup of $V$ then $G$ is finitely generated.
Proof. By replacing \( V \) by the vector subspace spanned by \( G \), we can assume without loss of generality that \( G \) spans \( V \). Using the isomorphism \( V \cong \mathbb{R}^n \), we can also assume without loss of generality that \( V = \mathbb{R}^n \) and that \( G \) contains the canonical basis. We consider the quotient map
\[
\pi : \mathbb{R}^n \to \mathbb{R}^n / \mathbb{Z}^n,
\]
where \( \mathbb{R}^n / \mathbb{Z}^n \) is endowed with the quotient topology. The quotient \( \mathbb{R}^n / \mathbb{Z}^n \) is compact, since it is homeomorphic to the \( n \)-torus. Further, one can easily verify that the map \( \pi \) is open. As \( \mathbb{Z}^n = \ker(\pi) \subseteq G \) we find \( G = \pi^{-1}(\pi(G)) \). Let \( \pi(x) \in \pi(G) \). As \( G \) is discrete we find an open subset \( U \) in \( \mathbb{R}^n \) such that
\[
\{x\} = U \cap G.
\]
Further
\[
\{\pi(x)\} = \pi(U) \cap \pi(G)
\]
and thus \( \pi(G) \) is discrete. Then, since \( G \) is closed and \( G = \pi^{-1}(\pi(G)) \), by the definition of the quotient topology \( \pi(G) \) is closed. Therefore \( \pi(G) \cong G / \mathbb{Z}^n \) is compact and discrete, hence finite. Since \( \mathbb{Z}^n \) and \( G / \mathbb{Z}^n \) are both finitely generated, it follows that \( G \) is finitely generated. □

**Proof (of theorem 2.5).** Let \( \phi \in \text{Hom}(E_1, E_2) \otimes_\mathbb{Z} \mathbb{Z}_l \), and suppose that \( \phi_l = 0 \). Let
\[
M \subseteq \text{Hom}(E_1, E_2)
\]
be some finitely generated subgroup with the property that \( \phi \in M \otimes_\mathbb{Z} \mathbb{Z}_l \). Then, with notation as in Lemma 2.6, the group \( M^{\text{div}} \) is finitely generated. Since \( M^{\text{div}} \) is torsion-free and therefore free, we find a \( \mathbb{Z} \)-basis
\[
\psi_1, \ldots, \psi_t \in \text{Hom}(E_1, E_2)
\]
of \( M^{\text{div}} \). Since \( \mathbb{Z}_l \) is flat, we have the natural inclusion
\[
M \otimes_\mathbb{Z} \mathbb{Z}_l \hookrightarrow M^{\text{div}} \otimes_\mathbb{Z} \mathbb{Z}_l.
\]
Thus, we can and write
\[
\phi = \alpha_1(\psi_1 \otimes 1) + \cdots + \alpha_t(\psi_t \otimes 1) \quad \text{with} \quad \alpha_1, \ldots, \alpha_t \in \mathbb{Z}_l.
\]
We fix some integer \( n \geq 1 \) and choose \( a_1, \ldots, a_t \in \mathbb{Z} \) such that \( a_i \) is congruent to the \( n \)’s component of \( \alpha_i \) modulo \( l^n \), i.e
\[
a_i \equiv \alpha_i \mod l^n.
\]
Let
\[
\psi := [a_1] \circ \psi_1 + \cdots + [a_t] \psi_t \in \text{Hom}(E_1, E_2).
\]
By the universal property of the projective limit we have the commutative diagram

$$
\begin{array}{ccc}
T_l(E_1) & \xrightarrow{\phi_l} & T_l(E_2) \\
\downarrow{\pi^1_n} & & \downarrow{\pi^2_n} \\
E_1[l^n] & \xrightarrow{\phi_n} & E_2[l^n]
\end{array}
$$

Then, since by [Sil86, III.4.2] and [Sil86, II.3] the multiplication-by-$l$-maps are surjective, the projection maps $\pi^1_n$ and $\pi^2_n$ are surjective. As $\phi_l = 0$ we get

$$0 = \phi_n(P) = \sum_{i=1}^r a_i \psi_i(P) = \psi(P) = 0 \quad \text{for all } P \in E_1[l^n].$$

It follows from [Sil86, III.4.11] that $\psi$ factors through $[l^n]$, so there is an isogeny

$$\lambda \in \text{Hom}(E_1, E_2) \quad \text{satisfying} \quad \psi = [l^n] \circ \lambda.$$ 

Then $\lambda$ lies in $M^{\text{div}}$, so there are integers $b_i \in \mathbb{Z}$ such that

$$\lambda = [b_1] \circ \psi_1 + \cdots + [b_t] \circ \psi_t.$$ 

Further, since the $\psi_i$’s form a $\mathbb{Z}$-basis for $M^{\text{div}}$, the fact that $\psi = [l^n] \circ \lambda$ implies that

$$a_i = l^n b_i,$$

and hence

$$\alpha_i \equiv 0 \mod l^n.$$ 

This holds for all $n$, so we conclude that $\alpha_i = 0$, and derive $\phi = 0$. \hfill \blacksquare

**Corollary 2.8.** Let $E_1/k$ and $E_2/k$ be elliptic curves and let $l \neq \text{char}(K)$ be a prime. Then

$$\text{Hom}(E_1, E_2)$$

is a free $\mathbb{Z}$-module of rank at most 4.

**Proof.** By definition we have

$$\text{rank}_\mathbb{Z} \text{Hom}(E_1, E_2) = \text{dim}_\mathbb{Q} \text{Hom}(E_1, E_2) \otimes_\mathbb{Z} \mathbb{Q}.$$ 

Further

$$\text{dim}_\mathbb{Q} \text{Hom}(E_1, E_2) \otimes_\mathbb{Z} \mathbb{Q} = \text{dim}_\mathbb{Q}_l \text{Hom}(E_1, E_2) \otimes_\mathbb{Z} \mathbb{Q} \otimes_\mathbb{Q} \mathbb{Q}_l$$

$$= \text{dim}_\mathbb{Q}_l \text{Hom}(E_1, E_2) \otimes_\mathbb{Z} \mathbb{Z}_l \otimes_\mathbb{Z}_l \mathbb{Q}_l$$

$$= \text{rank}_\mathbb{Z}_l \text{Hom}(E_1, E_2) \otimes_\mathbb{Z} \mathbb{Z}_l.$$
This implies that
\[ \text{rank}_\mathbb{Z} \text{Hom}(E_1, E_2) = \text{rank}_\mathbb{Z}_l \text{Hom}(E_1, E_2) \otimes \mathbb{Z}_l, \]
in the sense that if one is finite, then the other is finite and they are equal. Next, from theorem \[ \text{2.5}\] we have the estimate
\[ \text{rank}_\mathbb{Z}_l \text{Hom}(E_1, E_2) \otimes \mathbb{Z}_l \leq \text{rank}_\mathbb{Z}_l \text{Hom}(T_l(E_1), T_l(E_2)). \]
Finally, choosing a \( \mathbb{Z}_l \)-basis for \( T_l(E_1) \) and \( T_l(E_2) \), we see from proposition \[ \text{2.2}\] that
\[ \text{Hom}(T_l(E_1), T_l(E_2)) = M_2(\mathbb{Z}_l) \]
is the additive group of \( 2 \times 2 \) matrices with \( \mathbb{Z}_l \)-coefficients. The \( \mathbb{Z}_l \)-rank of \( M_2(\mathbb{Z}_l) \) is 4, which proves that \( \text{rank}_\mathbb{Z} \text{Hom}(E_1, E_2) \) is at most 4.

Now let
\[ \sum_{j_1}^{k_1} m_{j_1} \otimes \frac{1}{z_{j_1}}, \ldots, \sum_{j_n}^{k_n} m_{j_n} \otimes \frac{1}{z_{j_n}} \]
be a basis of the \( \mathbb{Q} \)-vector space \( \text{Hom}(E_1, E_2) \otimes \mathbb{Q} \) with \( n \leq 4 \). Let
\[ M := \langle m_{j_1}, \ldots, m_{k_1}, \ldots, m_{j_n}, \ldots, m_{k_n} \rangle \]
and let \( \phi \) be an arbitrary isogeny in \( \text{Hom}(E_1, E_2) \). We find an integer \( m \), which is at least 1, such that \( m(\phi \otimes 1) \) lies in \( M \otimes \mathbb{Z} \), so \( [m] \circ \phi \) lies in \( M \). This implies that
\[ M^{\text{div}} = \text{Hom}(E_1, E_2) \quad \text{and from lemma \[ \text{2.6}\] we derive that} \quad \text{Hom}(E_1, E_2) \text{ is finitely generated. Further Hom}(E_1, E_2) \text{ is torsion-free, hence free.} \]

\[ \textbf{Remark.} \] We say that an isogeny is \textit{defined over} \( K \) if it commutes with the action of the absolute Galois group \( \text{Gal}(\bar{K}|K) \). We denote the group of all isogenies defined over \( K \) by
\[ \text{Hom}_K(E_1, E_2). \]
Similarly, we can define
\[ \text{Hom}_K(T_l(E_1), T_l(E_2)) \]
to be the group of \( \mathbb{Z}_l \)-linear maps from \( T_l(E_1) \) to \( T_l(E_2) \) that commute with the action of \( \text{Gal}(\bar{K}|K) \) as given by the \( l \)-adic representation. Then we have a homomorphism
\[ \text{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_l \rightarrow \text{Hom}_K(T_l(E_1), T_l(E_2)), \]
and theorem \[ \text{2.5}\] tells us that this homomorphism is injective. It turns out that in many cases, it is an isomorphism.
**Theorem 2.10** (Isogeny Theorem). Let $E_1$ and $E_2$ be elliptic curves and let $l \neq \text{char}(K)$ be a prime. Then the natural map

$$\text{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_l \longrightarrow \text{Hom}_K(T_l(E_1), T_l(E_2))$$

is an isomorphism in the following two situations:

(a) $K$ is a finite field. (Tate)

(b) $K$ is a number field (Faltings)

**A Group Action**

Let $\mathcal{C}$ be a category with small Hom sets, $X$ an object of $\mathcal{C}$ and $G$ a group. A (left) group action of $G$ on $X$ is a group homomorphism

$$G \longrightarrow \text{Aut}_{\mathcal{C}}(X).$$

In the category $(\text{Set})$ of sets the datum of a group homomorphism from $G$ to $\text{Aut}_{(\text{Set})}(X)$ is equivalent to the datum of a map

$$G \times X \longrightarrow X$$

$$(g, x) \longmapsto g \cdot x$$

with the following properties:

i.) For all $x \in X$ we have $1 \cdot x = x$;

ii.) For all $x \in X$ and all $g, h \in G$ we have $(g \cdot h) \cdot x = g \cdot (h \cdot x)$.

In the category $(\text{Group})$ of groups the datum of a group homomorphism from $G$ to $\text{Aut}_{(\text{Group})}(M)$ is equivalent to the datum of a map

$$G \times M \longrightarrow M$$

$$(g, x) \longmapsto g \cdot x$$

with the following properties:

i.) For all $g \in G$ the map $g \cdot : M \longrightarrow M$ is a group homomorphism, i.e $g \cdot (m \cdot n) = g \cdot m \cdot g \cdot n$ for all $m, n \in M$ and $g \in G$;

ii.) For all $m \in M$ we have $1 \cdot m = m$;

iii.) For all $m \in M$ and all $g, h \in G$ we have $(g \cdot h) \cdot m = g \cdot (h \cdot m)$.

If $G$ is a group and $M$ is an abelian group, such that $G$ acts on $M$ in in the category $(\text{Group})$, then one calls $M$ a $G$-module.
References
